資料25

個人情報保護管理運営会議　付議事項

件名	ベビーシッター利用支援事業（一時預かり利用支援）に係る業務の委託について（委託内容の追加）

内容は別紙のとおり

要綱の根拠

◇第３条第１項第３号（業務委託）

（担当部課：子ども総合センター子ども家庭支援課）

事業の概要

事業名	ベビーシッター利用支援事業（一時預かり利用支援）
担当課	子ども家庭支援課
目　的	ベビーシッター利用支援事業につき、区民の利便性向上と業務の効率化を図るため。
対象者	0歳から満6歳に達する年度の末日までの間にある児童の保護者
事業内容	1　概要 日常生活上の突発的な事情等により、一時的にベビーシッターによる保育を必要とする保護者に対して保育利用料の一部を助成している。（令和５年度第１回個人情報保護管理運営会議承認済） 今般、区民の利便性向上を図るため、LoGo フォームによる電子申請を導入し、ベビーシッター利用支援事業助成金の効率的な交付手続を行う。ついては、申請者が LoGo フォームへ申請した内容について、委託事業者に確認及び集計を行わせることで、職員の負担を軽減し、業務の効率化を図る。（LoGo フォームによる電子申請の導入については、令和６年度第３回個人情報保護管理運営会議承認済） 2　個人情報保護管理運営会議への付議内容 （1）コールセンター業務 （2）申請書類の受付及び事前審査業務（申請の審査、助成決定は区が実施） （3）申請データ管理 （4）交付決定通知の送付 **（5）LoGo フォームへの電子申請内容の確認及び集計管理** 3　想定人数 約2,000人 ※個人情報の流れは、資料２５－１のとおり

別紙（業務委託）

◇業務委託（第３条第１項第３号）

件名　ベビーシッター利用支援事業（一時預かり利用支援）に係る業務の委託について（委託内容の追加）

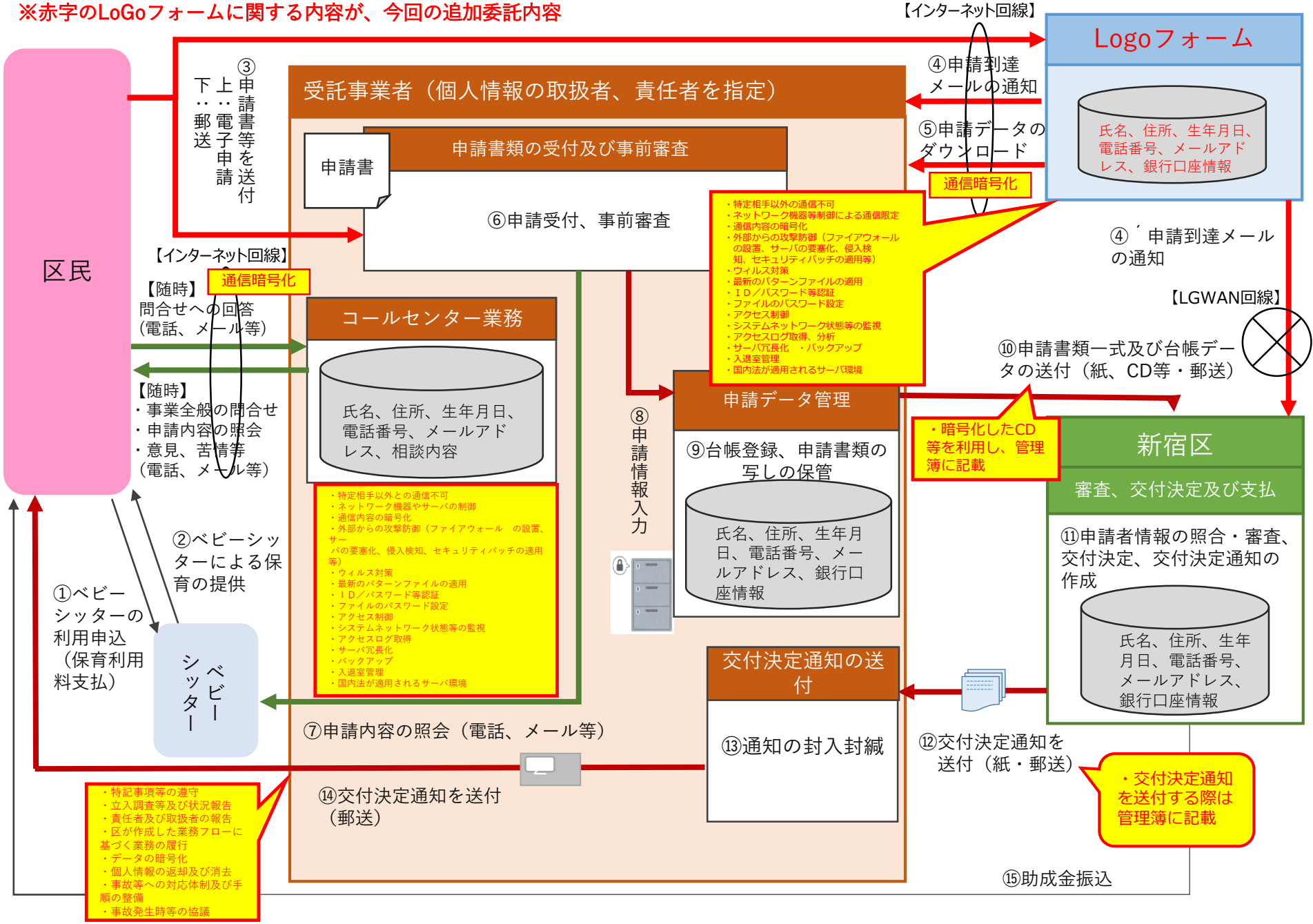
※太字ゴシック（下線）が、令和５年度第１回新宿区個人情報保護管理運営会議承認済の内容からの変更箇所

保有課（担当課）	子ども家庭支援課
登録業務の名称	ベビーシッター利用支援事業（一時預かり利用支援）
委託先	**株式会社バックスグループ（プライバシーマーク取得済）**
委託に伴い事業者に処理させる情報項目（だれの、どのような項目か）	《委託先に提供する項目、委託先に収集させる項目》 氏名、住所、生年月日、電話番号、メールアドレス、銀行口座情報、相談内容
処理させる情報項目の記録媒体	紙及び電磁的媒体（委託先のパソコン**、Logo フォーム**）
委託理由	事業を円滑に実施するため、助成の申請受付から交付決定までの事務や問合せへの対応等において、区の業務を補助するため。
委託の内容	（１）コールセンター業務 （２）申請書類の受付及び事前審査業務（申請の審査、助成決定は区が実施） （３）申請データ管理 （４）交付決定通知の送付 （５）**LoGo フォームへの電子申請内容の確認及び集計管理**
委託の開始時期及び期限	**令和６年７月２６日から令和７年３月３１日**（次年度以降も、同様の業務委託を行う。）
委託にあたり区が行う情報保護対策	別紙チェックリストのとおり
受託事業者に行わせる情報保護対策	別紙チェックリストのとおり

ベビーシッター利用支援事業（一時預かり利用支援）委託に係る個人情報の流れ

（資料２５－１）

※赤字のLoGoフォームに関する内容が、今回の追加委託内容



5　業務委託にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
委託にあたり区が行う情報保護対策【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、個人情報保護法及び新宿区情報セキュリティポリシーを遵守するよう指導する。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠するよう指導する。
	○	契約履行の間、特記事項に基づき立入り調査等を実施するとともに、委託先に対し速やかに状況報告をするよう指導する。
	○	取扱責任者及び取扱者をあらかじめ指定し、区に報告するよう指導する。
	○	全体の業務フローを作成し、委託先と共有する。
	○	個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化する。また、電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用して、手渡しで行うよう指導する。
	○	個人情報を手交する場合は、鍵付きカバン等を使用して運搬する。
	○	個人情報の受渡しにあたっては、管理簿に記載する。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにする。
	○	個人情報は、施錠できる金庫又はキャビネット等に保管する。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却し、電子データは消去するよう指導する。また、区に電子データの消去を行ったことの報告書を提出するよう指導する。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備し、委託先と緊急時の連絡体制や対応手順を確認する。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに委託先と今後の対応を協議する。
委託にあたり区が行う情報保護対策【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定する。
	○	通信内容は暗号化し、通信途上の個人情報の盗用、改ざん、成りすましを防止する。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御する。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用する。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止する。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定するとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底する。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得する。取得したログは、定期的に分析する。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備する。
	○	入退室管理等により情報資産の危殆化を防止する。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にする。

5　業務委託にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
委託事業者に行わせる情報保護対策【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、個人情報保護法及び新宿区情報セキュリティポリシーを遵守させる。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠させる。
	○	契約履行の間、特記事項に基づき立入り調査等を受けさせるとともに、委託先に対し速やかに状況報告をさせる。
	○	取扱責任者及び取扱者をあらかじめ指定させ、区に報告させる。
	○	区が作成した業務フローに基づき、業務を行わせる。
	○	個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化させる。電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用させ、手渡しで行わせる。
	○	個人情報を手交する場合は、鍵付きカバン等を使用して運搬させる。
	○	個人情報の受け渡しにあたっては、管理簿に記載させる。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにさせる。
	○	個人情報は、施錠できる金庫又はキャビネット等に保管させる。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却させ、電子データは消去させる。また、区に電子データの消去を行ったことの報告書を提出させる。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備させ、区と緊急時の連絡体制や対応手順を確認させる。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに区と今後の対応を協議させる。
委託事業者に行わせる情報保護対策【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定させる。
	○	通信内容は暗号化させ、通信途上の個人情報の盗用、改ざん、成りすましを防止させる。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じさせ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御させる。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用させる。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止させる。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定させるとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底させる。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得させる。取得したログは、定期的に分析させる。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備させる。
	○	入退室管理等により情報資産の危殆化を防止させる。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にさせる。